QUALYS SECURITY CONFERENCE 2019

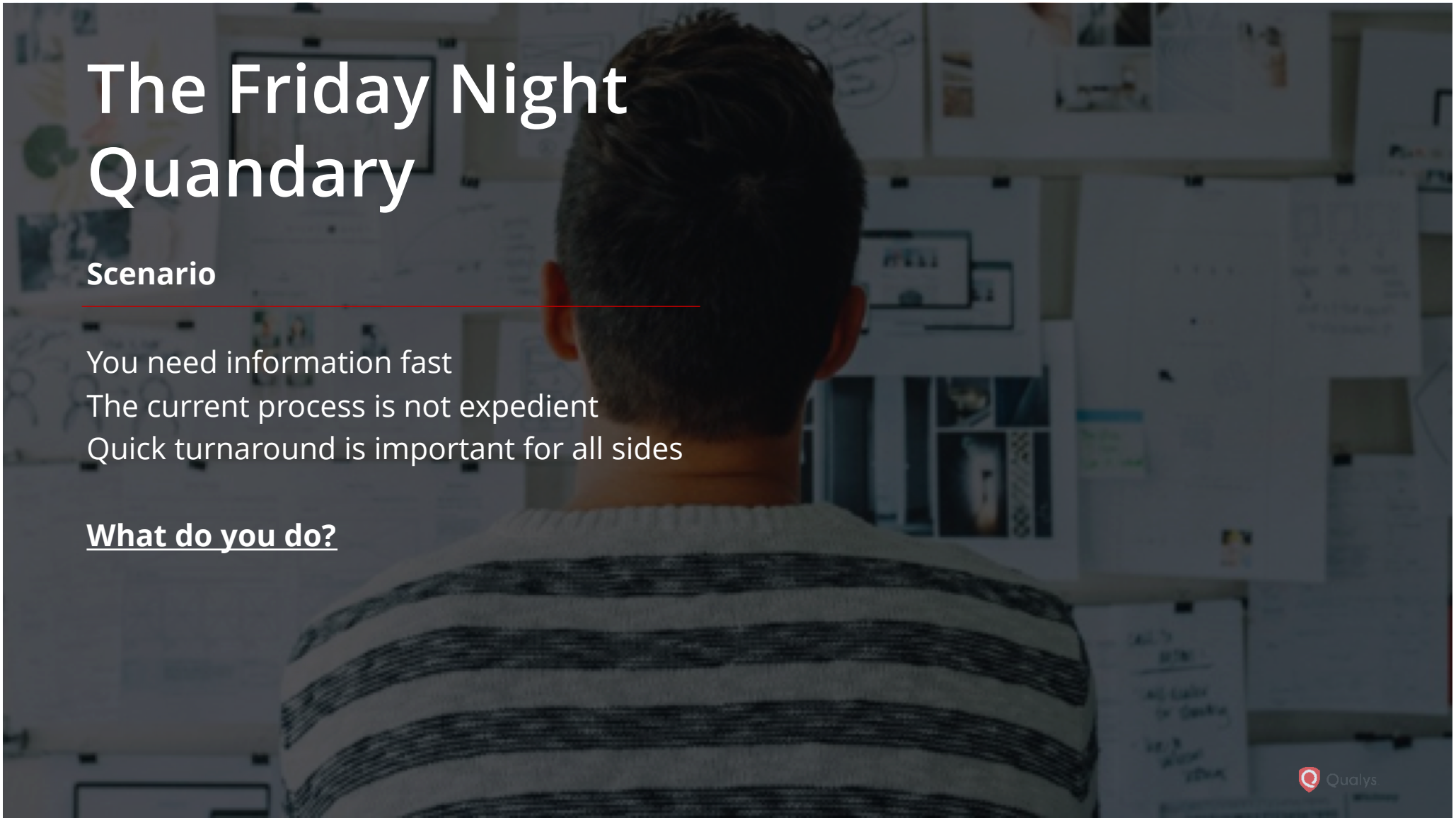
Building an Enterprise ITAM for IT & Security

Chris Rodgers
Director of Product Management, Qualys, Inc.

Agenda

Friday Night Quandary
Challenges and Goals
Process
Case Study

Qualys.



The Friday Night Quandary

Scenario

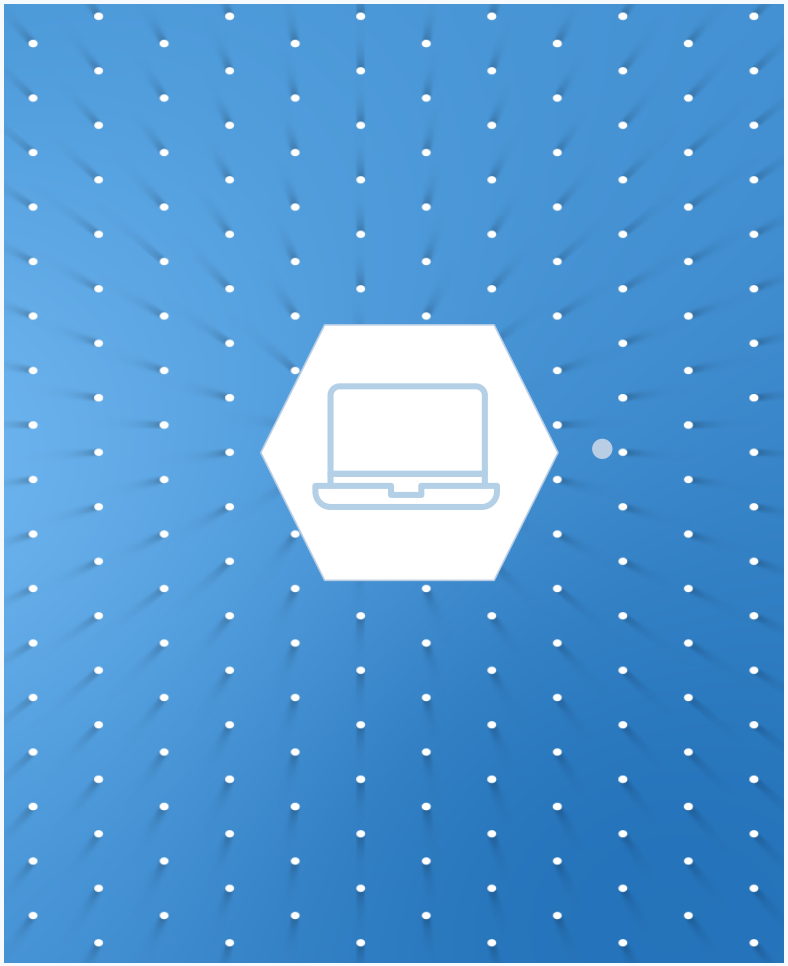
You need information fast
The current process is not expedient
Quick turnaround is important for all sides

What do you do?

Qualys

Primary Challenges

Lack of Focus
Simplification Needed
Data Clarity



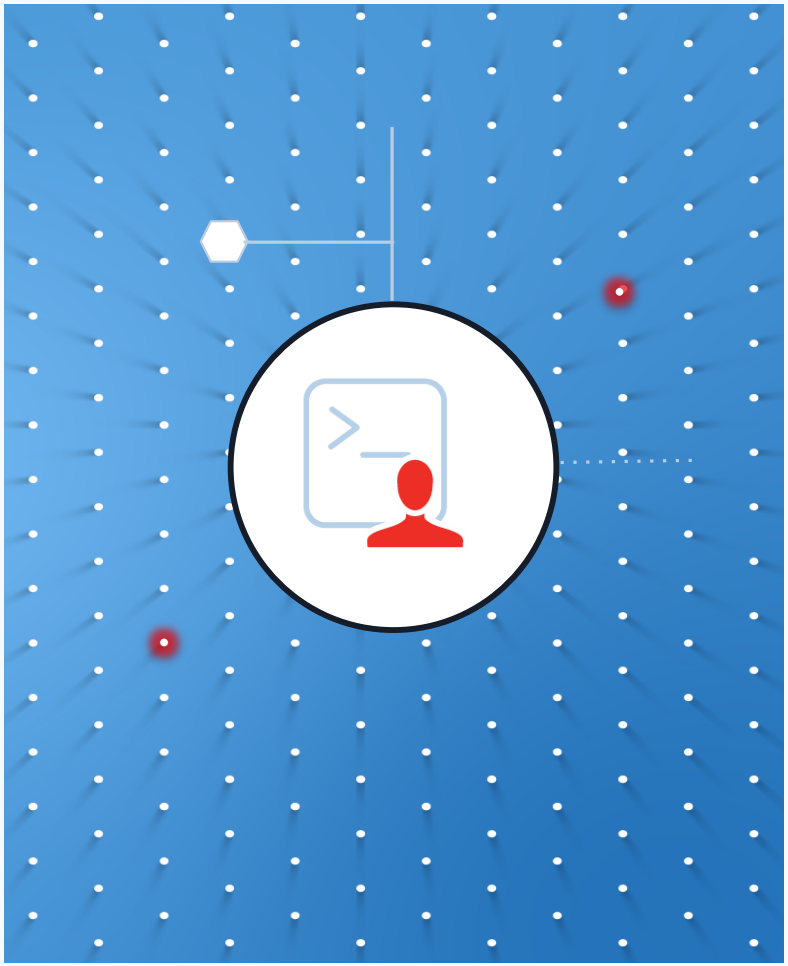
Principles I am Looking For?

Ownership Who gets what?

Categorization Once they get it, what do they do with it?

Timelines – What is truly new vs older?

Prioritization - After everything is said and done, what matters most?



Goals

Qualys.

Asset Management: General

Active / EOL / EOS Breakdown

Active – Business as usual

EOL – Amortize funds for replacement

EOS – Replace system

Data Centers – Based on IP

Grouping – Operating System & Business Units / Owners

Focus, Simplification, & Clarity :

**By separating the Active, EOL, & EOS*, we can break down different actions for different groups.

**By identifying the datacenters and groups*, we can take the raw data and work outside of the UI to get quick AD Hoc details.

Asset Management: Indexing

<u>Over the course of the first 3 months of the program, we identified:</u>

- IP's and DNS listings belong to each group.
- Operating system lifecycles
  - If an operating system should be considered Remediable or Replaceable at our discretion.
- If an IP range is Public or Private
- Baseline readings to compare vulnerability data from certain timeframes
- Identify what IP's existed at a certain point in time vs. current point.

<u>Focus, Simplification, & Clarity</u> :
By utilizing indexing groups, we are able to bring in data and create desired tags to add for the report. This allows us to filter vulnerabilities based on characterizations.

Prioritization Modeling

Each organization has important data

- Datacenters
- Assets with Intellectual Property
- Revenue Generating Assets
- Social Assets (workstations, kiosks, etc.)

For us, we chose to keep the process simple

- Location component based on value of the data
- CVSS Score
- Severity Rating
- Days outstanding
- Exploitability RTI's

Focus, Simplification, & Clarity :
We created a ranking process unique to our needs. This gave each team a simple, clear and focused plan of attack.

Time Stamping Modifications

Working with Timestamps can be tricky.

With Alteryx, we are able to take the timestamp and parse it and create days since categories where we have a tangible number outside of the timestamp.

Such as “Days since last scanned / Days since first scanned”

We can create buckets make filtering easy.

Focus, Simplification, & Clarity :
By creating days since categories, filtering ages becomes a simple, scalable task. It identifies how many days have lapsed from when the scan report was run to the days since identification.

Parsing

System parses are needed to provide a full and complete picture

In Qualys, VM Operating systems granular. (Windows 2008 R2)

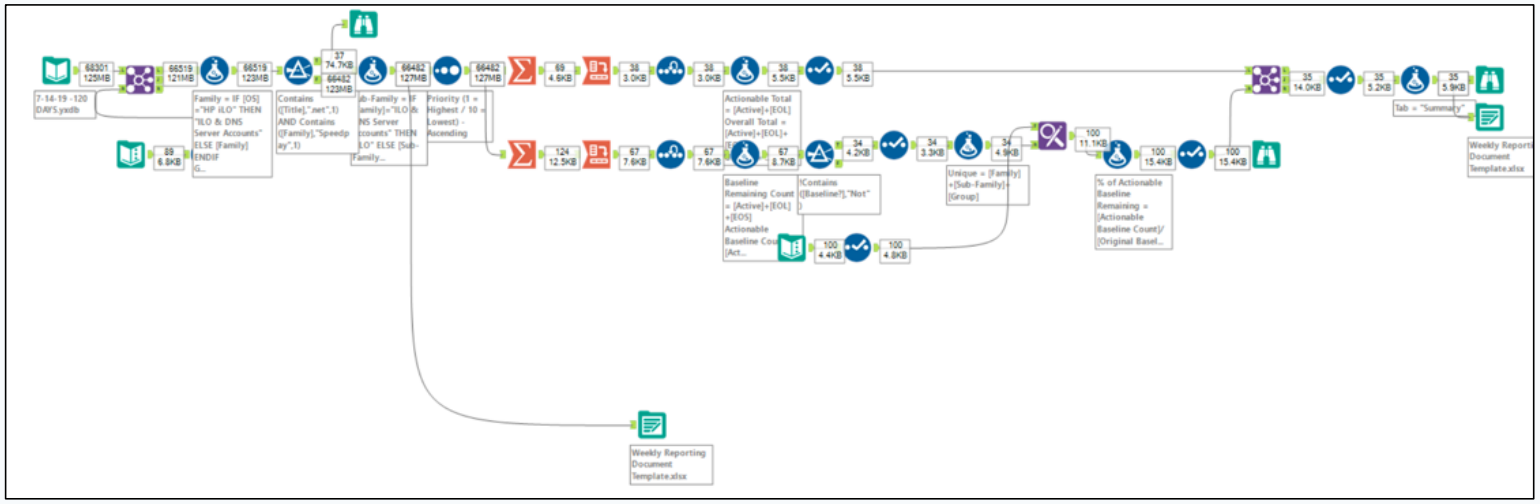
- In the event that we are needing to view the highest level we can easily (Windows)
- In the event that we want to group by the operating system name, that is also an option. (Windows 2000)

DNS most often is a joining of the Host / Domain.

- Simple parsing allows us to break these two items up and report separately.

Focus, Simplification, & Clarity :
By parsing datasets, we can get specific data that may be inherent in the base data from Qualys.

What Does the Workflow Look Like?



THE PROCESS IS SIMPLE BUT DETAILED

Qualys.

Outcome

- With Alteryx, we were able to process modifications in less than 1 minute.
- Pushed out a simple Excel sheet that had ownership parsed and tabbed for simple and clear usages.
- Created a historical repository of all auditable vulnerabilities.
- We were able to reduce vulnerabilities by 85%.

This was all because we simplified the system and provided clear and actionable results in the language my team spoke.

Qualys.

Case Study: 2019

Researchers find stealthy MSSQL server backdoor developed by Chinese cyberspies

ESET finds new "skip-2.0" backdoor developed by Chinese cyber-espionage group, targeting MSSQL v12 and v11.

By Catalin Cimpanu for Zero Day | October 21, 2019 -- 09:30 GMT (02:30 PDT) | Topic: Security

https://www.zdnet.com/article/researchers-find-stealthy-mssql-server-backdoor-developed-by-chinese-cyberspies/

Qualys.

SQL Demo

Thank You

Christopher Rodgers
crodgers@qualys.com